МАТЕМАТИЧЕСКАЯ ЛОГИКА, АЛГЕБРА, ТЕОРИЯ ЧИСЕЛ И ДИСКРЕТНАЯ МАТЕМАТИКА

УДК 510.65

О МОНОИДЕ С РАЗРЕШИМОЙ ТЕОРИЕЙ КОНЕЧНЫХ ПОДМНОЖЕСТВ

Дудаков С.М.
Тверской государственный университет, г. Тверь
Национальный исследовательский университет «Высшая школа экономики», г. Москва

Поступила в редакцию 25.04.2024, после переработки 17.07.2024.

В наших предыдущих работах мы продемонстрировали, что теория конечных подмножеств различных ассоциативных алгебр позволяет интерпретировать элементарную арифметику, в частности, она неразрешима. Например, это было показано для любых бесконечных абелевых групп. Возникает естественный вопрос: можно ли обобщить этот результат на более широкий класс алгебр, скажем, все коммутативные моноиды. В некоторых случаях нами ответ тоже получен ранее: для коммутативных моноидов с сокращением, имеющим элемент бесконечного порядка или произвольных абелевых групп. Сейчас же мы продемонстрируем, что не для всяких коммутативных моноидов это верно. Более того, мы дадим описание конструкции, которая позволяет строить такого рода системы из разного рода исходных алгебр. Вместе с тем, будут указаны и некоторые границы её применимости.

Ключевые слова: алгебра подмножеств, алгоритмическая разрешимость, автоматная система.

Вестник ТвГУ. Серия: Прикладная математика. 2024. № 2. С. 27–38.
https://doi.org/10.26456/vtpmk708

Введение

В любой алгебре операции можно перенести с отдельных элементов на их всевозможные или только конечные подмножества. Таким образом получаются новые алгебры исходной сигнатуры. Мы занимаемся изучением алгебр, построенных, как подмножества коммутативных моноидов.

Такого рода исследования начались в середине XX в. (см. [8]). Конструкция алгебры подмножеств во многих случаях естественна. Например, таким образом можно перейти от операций над словами к операциям над языками (см. [5]). Некоторые известные математические проблемы тоже можно сформулировать в терминах действий над подмножествами. Скажем, тернарная и бинарная проблемы

Гольдбаха могут быть сформулированы как $O = P + P + P$ и $E = P_1 + P_1$ соответственно. Здесь O — множество нечётных натуральных чисел, начиная с 7; E — множество чётных натуральных чисел, начиная с 6; P и P_1 — множества всех простых и нечётных простых чисел соответственно.

Ранее мы уже получили ряд результатов о выразительной силе теории всевозможных или только конечных подмножеств. В некоторых случаях, для специального вида унаров, может наблюдаться даже упрощение теории конечных подмножеств по сравнению с теорией исходного унара (см. [1]). Но для нетривиальных алгебр с бинарной операцией мы наблюдали противоположную картину. Например, уже для простейшего моноида $(\omega, +, 0)$, аддитивной алгебры натуральных чисел, теория алгебры конечных подмножеств алгоритмически эквивалентна элементарной арифметике, а теория алгебры всех подмножеств — арифметике второго порядка (см. [3]). Ещё одним таким результатом является возможность интерпретации элементарной арифметики в теории алгебры конечных подмножеств бесконечных абелевых групп (см. [4, 6]).

Последний результат может быть перенесён на некоторые моноиды, а именно — на моноиды с сокращением, имеющие элемент бесконечного порядка (см. [4]). Возникает естественный вопрос о возможности обобщения этих результатов на более широкий круг бесконечных моноидов или, более общо, полугрупп: верно ли, что для всех таких систем алгебра подмножеств позволит интерпретировать элементарную арифметику?

В самом широком смысле этот результат тривиально неверен. Например, в полугруппе с нулевой операцией, то есть $x + y = 0$ для любых x и y, для произвольных непустых подмножеств мы точно также получим $X + Y = \{0\}$, поэтому полугруппа подмножеств элементарно эквивалентна исходной (если она, конечно, бесконечна).

В настоящей работе мы указываем некоторые примеры построения нетривиальных полугрупп и моноидов, для которых полугруппы или моноиды подмножеств будут иметь разрешимую теорию, причём это касается как конечных подмножеств, так и произвольных. Для случая алгебры конечных подмножеств мы получим автоматную систему (см. [2]), а алгебра всех подмножеств будет интерпретироваться в монадической теории второго порядка с двумя следованиями S2S, разрешимость которой показана в знаменитой работе [7]. Вместе с тем мы укажем и границы применимости этой конструкции: если исходные алгебры будут образовывать неограниченно возрастающую цепь, то дизъюнктное объединение этой цепи будет системой, теория конечных подмножеств которой снова оказывается эквивалентной элементарной арифметике и, следовательно, неразрешимой.

1. Определения

Как обычно для коммутативных моноидов мы будем считать, что бинарная операция обозначается знаком плюс, а нейтральный элемент — нулём.

Для каждой алгебры $\mathfrak{A}$ можно рассмотреть алгебру её всех $\exp^* \mathfrak{A}$ или только конечных $\exp \mathfrak{A}$ непустых подмножеств с операциями типа

$$f(X_1, \ldots, X_n) = \{f(a_1, \ldots, a_n) : a_1 \in X_1, \ldots, a_n \in X_n\}.$$

Исключение пустого множества оправдано тем, что в алгебрах $\exp^*_\varnothing \mathfrak{A}$ и $\exp_\varnothing \mathfrak{A}$, содержащих пустое множество, оно определимо при наличии хотя бы одной операции f местности два или больше:

$$X = \varnothing \equiv (\forall Y) f(X, Y, \ldots, Y) = X.$$

С другой стороны, если аргументы операции f не являются пустыми множествами, то и результат пустым множеством не будет. Таким образом, непустые множества образуют в $\exp^*_\varnothing \mathfrak{A}$ и $\exp_\varnothing \mathfrak{A}$ определимые подалгебры, и наоборот, теория алгебр $\exp^*_\varnothing \mathfrak{A}$ и $\exp_\varnothing \mathfrak{A}$ интерпретируется в $\exp^* \mathfrak{A}$ и $\exp \mathfrak{A}$ соответственно. Значит, исключение пустого множества не влияет на выразительную силу языка логики первого порядка, когда $\mathfrak{A}$ является группоидом и, в частности, моноидом.

Мы в нашей работе будем рассматривать два вида алгебр.

Алгебры первого типа являются усложнением моноида $\Omega = (\omega, \max, 0)$ — множества натуральных чисел с операцией взятия максимума двух элементов и нулём в качестве нейтрального. Пусть $\mathfrak{A}$ — любая алгебра. Мы будем рассматривать декартово произведение $\Omega \times \mathfrak{A}$.

Лемма 1. *Для любого (коммутативного) моноида/полугруппы $\mathfrak{A}$ алгебра $\Omega \times \mathfrak{A}$ является (коммутативным) моноидом/полугруппой.*

Доказательство. Моноиды и полугруппы образуют многообразие, а каждое многообразие замкнуто относительно декартовых произведений. □

Второй тип алгебр получается так. Декартово произведение — это множество пар (u, a), где $u \in \omega$ и $a \in \mathfrak{A}$. При этом

$$(u_1, a_1) + (u_2, a_2) = (\max(u_1, u_2), a_1 + a_2). \tag{1}$$

Но можно для каждого u вместо одной и той же алгебры $\mathfrak{A}$ брать свою собственную $\mathfrak{A}_u$, важно лишь, чтобы они образовывали (нестрого) возрастающую цепь: $\mathfrak{A}_u \subseteq \mathfrak{A}_v$ при $u \leqslant v$. Формальное определение (1) операции $+$ останется тем же самым. Такая конструкция называется дизъюнктным объединением $\bigsqcup\limits_{u \in \omega} \mathfrak{A}_u$. Очевидно, что декартово произведение $\Omega \times \mathfrak{A}$ будет частным случаем дизъюнктного объединения, когда цепь состоит из одного и того же элемента $\mathfrak{A}$.

По аналогии с предыдущей будет верна

Лемма 2. *Для любой (нестрого) возрастающей цепи (коммутативных) моноидов $\mathfrak{A}_u$, $u \in \omega$, дизъюнктное объединение $\bigsqcup\limits_{u \in \omega} \mathfrak{A}_u$ является (коммутативным) моноидом.*

Доказательство. Ассоциативность непосредственно вытекает из определения (1) операции $+$. Нулём будет $(0, 0_0)$, где 0_0 — нейтральный элемент моноида $\mathfrak{A}_0$. □

2. Автоматность алгебры конечных подмножеств

Для доказательства разрешимости теорий моноидов типа $\exp \mathfrak{A}$ в настоящей статье мы будем применять метод автоматных систем.

Определение 1 (см. [2]). *Пусть $\mathfrak{A}$ — алгебраическая система сигнатуры Σ. Система $\mathfrak{A}$ называется* автоматной, *если существует алфавит Ξ, не содержащий символа Λ, и разнозначная функция $h : \mathfrak{A} \to \Xi^*$ (из $\mathfrak{A}$ в слова алфавита Ξ) такие, что для любого сигнатурного символа P множество слов*

$$h(P^{\mathfrak{A}}) = \{\langle h(a_1), \ldots, h(a_n)\rangle : (a_1, \ldots, a_n) \in P^{\mathfrak{A}}\},$$

а также множество значений функции h, образуют автоматный язык. Здесь с помощью $\langle h(a_1), \ldots, h(a_n)\rangle$ обозначено слово α в алфавите $(\Xi \cup \{\Lambda\})^n$, длина которого равна максимуму длин слов $h(a_j)$, и в котором i-я буква $\alpha^{(i)}$ имеет вид $(a_1^{(i)}, \ldots, a_n^{(i)})$, где $a_j^{(i)}$ — i-я буква слова $h(a_j)$, если его длина меньше i, или Λ в противном случае. Здесь и далее мы всегда считаем, что нумерация букв в словах и бесконечных последовательностях начинается с нуля.

Например,

$$\langle 001, 01, 1011\rangle = (0,0,0)(0,1,0)(1,\Lambda,1)(\Lambda,\Lambda,1).$$

Главным результатом об автоматных системах является следующее утверждение.

Теорема 1 (см. [2]). *Любая автоматная система имеет алгоритмически разрешимую теорию.*

Для начала продемонстрируем, как метод автоматных систем можно использовать для доказательства разрешимости алгебры конечных подмножеств.

Пример 1. Пусть $\Omega = (\omega, \max, 0)$ — моноид натуральных чисел с операцией взятия максимума. Тогда $\exp\Omega$ будет автоматной системой. В самом деле, определим кодирующую функцию h следующим образом: $h(X)$ – это слово в алфавите $\mathbb{B} = \{0,1\}$ длины $1 + \max X$, в котором i-й символ равен 1 тогда и только тогда, когда $i \in X$. Тогда нейтральный элемент $\{0\}$ моноида $\exp\Omega$ кодируется словом «1», а автомат, проверяющий условие $X + Y = Z$, выглядит так: мы просто проверяем, что в слове $h(Z)$ стоит единица на позиции i при выполнении хотя бы одного из двух условий: в слове $h(X)$ уже встретилась единица на позиции $j \le i$ и в слове $h(Y)$ на позиции i стоит единица, либо наоборот, в слове $h(Y)$ уже встретилась единица на позиции $j \le i$ и в слове $h(X)$ на позиции i стоит единица.

Теорема 2. *Для любого конечного моноида $\mathfrak{A}$ моноид $\exp(\Omega \times \mathfrak{A})$ является автоматной системой и, в частности, он имеет разрешимую теорию.*

Доказательство. Предположим, что моноид $\mathfrak{A} = (A, +, 0)$ содержит N элементов: $\mathfrak{A} = \{a_0 = 0, \ldots, a_{N-1}\}$. Закодируем элемент X моноида $\exp(\Omega \times \mathfrak{A})$ словом $h(X)$ в алфавите $\mathbb{B} = \{0,1\}$ следующим образом: единица на позиции $uN + p$, где $p = 0, \ldots, N-1$, стоит тогда и только тогда, когда $(u, a_p) \in X$. Длина слова $h(X)$ будет равна

$$N(1 + \max\{u : (u, a_p) \in X \text{ для некоторого } p\}).$$

Таким образом, для кодирования используются слова в алфавите $\mathbb{B}$, длина которых кратна N и среди последних N символов есть хотя бы одна единица. Такие слова образуют автоматный язык.

Нуль моноида $\exp(\Omega\times\mathfrak{A})$ — это пара $(0,0)$, которая кодируется словом «10^{N-1}».

Автомат, проверяющий условие $X+Y=Z$, должен будет иметь состояния вида (α,β), где α и β — слова длины N в алфавите $\mathbb{B}$. Единица в словах α и β на p-й позиции будет означать, что уже встретился элемент вида (u,a_p) в слове $h(X)$ или $h(Y)$ соответственно. Автомат должен будет проверять, что в слове $h(Z)$ стоят единицы там и только там, где они соответствуют элементам $\mathfrak{A}$, которые могут быть получены из элементов текущего $\mathfrak{A}$ и предыдущих.

Точнее, недетерминированный автомат $\mathfrak{N}$ может быть построен следующим образом. Автомат $\mathfrak{N}$ содержит всевозможные команды вида

$$\begin{gathered}(\alpha,\beta),\epsilon\to(\alpha,\beta,\epsilon,\epsilon,\epsilon);\\ (\alpha,\beta,\gamma_1,\gamma_2,\gamma_3),(\sigma_1,\sigma_2,\sigma_3)\to(\alpha,\beta,\gamma_1\sigma_1,\gamma_2\sigma_2,\gamma_3\sigma_3);\\ (\alpha,\beta,\delta_1,\delta_2,\delta_3),\epsilon\to(\alpha_*,\beta_*).\end{gathered}\tag{2}$$

Здесь $\alpha,\beta,\alpha_*,\beta_*,\delta_1,\delta_2,\delta_3\in\mathbb{B}^N$, $\alpha_*=\alpha\vee\delta_1$, $\beta_*=\beta\vee\delta_2$ (с помощью $\vee$ мы обозначили побитовую дизъюнкцию), $\gamma_1,\gamma_2,\gamma_3\in\mathbb{B}^p$, $p<N$, $|\gamma_1|=|\gamma_2|=|\gamma_3|$, ϵ — пустое слово, $\sigma_1,\sigma_2,\sigma_3\in\mathbb{B}$. Начальным будет состояние $(0^N,0^N)$, а принимающими будут все состояния вида (α,β). Команды (2) включаются только при выполнении следующего условия для всех $p=0,\ldots,N-1$:

$$\delta_3^{(p)}=1\iff\bigvee_{a_r+a_q=a_p}\bigl((\alpha_*^{(r)}=1\wedge\delta_2^{(q)}=1)\vee(\delta_1^{(r)}=1\wedge\beta_*^{(q)}=1)\bigr).$$

Таким образом, если третье слово кодирует Z, которое не может быть получено из первых двух слов, кодирующих X и Y, то автомат $\mathfrak{N}$ не будет содержать команду вида (2) и не сможет вернуться в принимающее состояние вида (α,β). □

3. Интерпретация алгебры всех подмножеств в S2S

Для доказательства разрешимости алгебры всех подмножеств построенных систем мы применим иной метод. Способ кодирования элементов X систем $\exp^*(\Omega\times\mathfrak{A})$ в принципе будет тем же, что и для $\exp(\Omega\times\mathfrak{A})$, но теперь вместо конечных слов мы будем рассматривать бесконечные последовательности символов: если моноид $\mathfrak{A}$ содержит N элементов $a_0,\ldots,a_{N-1}$, то единица на позиции $uN+p$, где $p=0,\ldots,N-1$, стоит тогда и только тогда, когда $(u,a_p)\in X$.

Напомним, что монадическая теория второго порядка с двумя следованиями (S2S) может быть определена как монадическая теория второго порядка алгебраической системы, состоящей из конечных слов в алфавите $\mathbb{B}$ в сигнатуре с двумя унарными операциями $\cdot0$ и $\cdot1$, означающими приписывание к слову нуля и единицы соответственно. Как показано в знаменитой работе М. Рабина [7], теория S2S разрешима. Поэтому, проинтерпретировав теории систем типа $\exp^*(\Omega\times\mathfrak{A})$ в S2S, мы докажем и их разрешимость тоже.

Теорема 3. *Для конечного моноида $\mathfrak{A}$ теория алгебры $\exp^*(\Omega\times\mathfrak{A})$ интерпретируется в* S2S *и поэтому разрешима.*

Доказательство. Сразу заметим, что в S2S определимо пустое слово ϵ, чем мы далее будем пользоваться:

$$x = \epsilon \equiv (\forall y)(x \neq y \cdot 1 \wedge y \neq y \cdot 0).$$

Неформально говоря, мы каждую последовательность X в алфавите $\mathbb{B}$ будем интерпретировать как множество всех её префиксов. Такого типа множества X выделяются с помощью формулы

$$\begin{aligned}\mathrm{Seq}(X) \equiv X(\epsilon) \wedge \\ \wedge (\forall x)(X(x) \to (X(x \cdot 1) \vee X(x \cdot 0)) \wedge \neg(X(x \cdot 1) \wedge X(x \cdot 0))) \wedge \\ \wedge (\forall x)(X(x \cdot 1) \vee X(x \cdot 0) \to X(x)),\end{aligned}$$

то есть вместе с любым словом содержится ровно один его последователь, а вместе с любым непустым словом — наибольший из его собственных префиксов. Это будет областью интерпретации. Здесь и до конца доказательства строчными буквами будут обозначаться переменные первого порядка, а заглавными — второго.

Далее нам потребуется формула, говорящая, что слово x имеет вид $y\mathbb{B}^k$, то есть x получено из y приписыванием ровно k символов:

$$x = y\mathbb{B}^k \equiv \bigvee_{\sigma \in \mathbb{B}^k} x = y \cdot \sigma^{(1)} \cdots \sigma^{(k)}.$$

Следующий шаг — определить, что слово x имеет вид $y(\mathbb{B}^k)^*$ для некоторого фиксированного k:

$$\begin{aligned}x = y(\mathbb{B}^k)^* \equiv (\exists Z)\big[Z(y) \wedge Z(x) \wedge \\ \wedge (\forall t)\big(Z(t) \to (\exists! s)(s = t\mathbb{B}^k \wedge Z(s))\big) \wedge \\ \wedge (\forall t)\big(Z(t) \wedge t \neq y \to (\exists s)(t = s\mathbb{B}^k \wedge Z(s))\big)\big].\end{aligned}$$

Здесь мы использовали стандартное логическое обозначение $(\exists! s)$ — существует единственный s.

Используя последнюю формулу, можно записать условие, что длина слова x кратна k: $x = \epsilon(\mathbb{B}^k)^*$.

Для интерпретации в S2S теории моноида $\exp^*(\Omega \times \mathfrak{A})$ нам будет достаточно определить нейтральный элемент $(0, 0_0)$ и операцию $+$. Первое интерпретируется как последовательность, состоящая из одной единицы и следующих за ней нулей:

$$X = (0,0) \equiv \mathrm{Seq}(X) \wedge X(\epsilon \cdot 1) \wedge (\forall x)(X(x) \wedge x \neq \epsilon \to X(x \cdot 0)).$$

Для интерпретации сложения нужно сказать, что единица на позиции $uN + p$ стоит тогда и только тогда, когда a_p получается как $a_r + a_q$, причём одно из них принадлежит $\mathfrak{B}_u$, а другое — $\mathfrak{B}_v$ для какого-то $v \leq u$:

$$\begin{aligned}X + Y = Z \equiv \mathrm{Seq}(X) \wedge \mathrm{Seq}(Y) \wedge \mathrm{Seq}(Z) \wedge (\forall z)\Big[Z(z \cdot 1) \leftrightarrow \\ \leftrightarrow (\exists x, y, s, t)\Big(X(x \cdot 1) \wedge Y(y \cdot 1) \wedge t = (\mathbb{B}^N)^* \wedge s = t(\mathbb{B}^N)^* \wedge \\ \wedge \bigvee_{a_p = a_r + a_q} \Big[z = s\mathbb{B}^p \wedge \big((x = s\mathbb{B}^r \wedge y = t\mathbb{B}^q) \vee (x = t\mathbb{B}^r \wedge y = s\mathbb{B}^q)\big)\Big]\Big)\Big]. \quad \square\end{aligned}$$

4. Обобщения

Естественный вопрос, который возникает — можно ли в рассмотренных нами конструкциях перейти к рассмотрению исходных алгебр неограниченной мощности? Естественным обобщением алгебры типа $\Omega\times\mathfrak{A}$ будет такое. Пусть $\mathfrak{A}_u$, $u \in \omega$, — возрастающая цепь конечных моноидов: $\mathfrak{A}_u \subsetneq \mathfrak{A}_{u+1}$. Тогда дизъюнктное объединение $\mathfrak{B} = \bigsqcup\limits_{u\in\omega} \mathfrak{A}_u$ состоит из пар вида (u, a), где $a \in \mathfrak{A}_u$, а операции выполняются естественным образом: $(u, a_u) + (v, a_v) = (\max(u, v), a_u + a_v)$. Но уже такая конструкция приводит к неразрешимости теории конечных подмножеств.

Теорема 4. *Пусть $\mathfrak{A}_u$, $u \in \omega$, $\mathfrak{A}_u \subsetneq \mathfrak{A}_{u+1}$ — возрастающая цепь конечных абелевых групп. Тогда в теории конечных подмножеств дизъюнктного объединения $\mathfrak{B} = \bigsqcup\limits_{u\in\omega} \mathfrak{A}_i$ интерпретируется теория конечных подмножеств (обычного) объединения цепи $\mathfrak{A} = \bigcup\limits_{u\in\omega} \mathfrak{A}_u$. Поэтому теория алгебры $\exp\mathfrak{B}$, как и теория алгебры $\exp\mathfrak{A}$, допускает интерпретацию элементарной арифметики и, следовательно, неразрешима (см. [6]).*

Доказательство. Сначала предположим, что мы уже смогли построить формулу $\mathrm{Zero}_1(Z)$, которая среди всех элементов моноида $\exp\mathfrak{B}$ выделяет элементы вида $\{0_u\}$, где 0_u — нейтральный элемент какой-то группы $\mathfrak{A}_u$. Далее в доказательстве с помощью нижнего индекса a_u мы будем обозначать номер группы $\mathfrak{A}_u$, из которой этот элемент взят.

Тогда интерпретация теории системы $\exp\mathfrak{A}$ в теории системы $\exp\mathfrak{B}$ будет устроена так. Область интерпретации ничем не ограничена, то есть содержит все элементы $\exp\mathfrak{B}$. Равенство $X = Y$ интерпретируется следующей формулой:

$$(\exists Z)(\mathrm{Zero}_1(Z) \wedge X + Z = Y + Z).$$

Иными словами, мы можем «сдвинуть» все элементы множеств X и Y в одну $\mathfrak{A}_u$ так, чтобы они совпали. Тогда, нетрудно заметить, что любое конечное непустое множество $S \subseteq \mathfrak{A}$ будет соответствовать каждому множеству, состоящему из тех же элементов, но возможно, в разных $\mathfrak{A}_u$. Наконец, сложение $X + Y = S$ интерпретируется формулой

$$(\exists Z)(\mathrm{Zero}_1(Z) \wedge (X + Z) + (Y + Z) = S + Z).$$

Здесь мы опять «сдвигаем» все элементы, входящие в формулу в то $\mathfrak{A}_u$, в котором это сложение можно корректно выполнить. Это тоже соответствует сложению конечных подмножеств в $\mathfrak{A}$.

Таким образом, нашей главной задачей является построение формулы Zero_1.

Сначала укажем формулу $\mathrm{Zero}_M(X)$, говорящую, что X состоит из одного или нескольких 0_u для каких-то u:

$$\mathrm{Zero}_M(X) \equiv X + X = X \wedge (\forall Y)(X + Y = X \to Y + Y = Y).$$

Нетрудно видеть, что здесь говориться: сам X и все нейтральные для него элементы являются идемпотентами.

Если $X = \{0_u : u \in I\}$, то, очевидно, $X + X = X$. Далее, если $X + Y = X$, то Y тоже должен содержать только 0_v для каких-то $v \in \omega$, иначе получим $0_u + a_v = a_{\max(u,v)} \neq 0_w$ для любых $u, v, w \in \omega$ и ненулевого a, то есть $X + Y \neq X$. Но тогда $Y + Y = Y$.

Теперь покажем обратное, пусть выполнено $\mathrm{Zero}_M(X)$. Допустим, что X содержит некоторый ненулевой элемент $a_u \in \mathfrak{A}_u$. Если X содержит 0_v для $v < u$, то выбрав наименьший из таких v мы можем построить $Y = \{0_v, a_u\}$, для которого

$$X = X + \{0_v\} \subseteq X + Y \subseteq X + X = X,$$

то есть $X + Y = X$, хотя, очевидно, Y идемпотентом не является, так как $a_u + a_u \neq a_u$ (в группе нет ненулевых идемпотентов).

Если такого v не существует, то возьмём $Y = \{a_u\}$. Поскольку группа $\mathfrak{A}_u$ является конечной, то $-a = (n-1)a$, где n — порядок a_u. Поэтому получаем $-a = (n-1)a \in (n-1)X = X$. Значит, для любого $b_v \in X$ получаем $u \leqslant v$, $b_v - a_u \in X + X = X$ и, следовательно, $X \subseteq Y + X$. Обратное включение получается из $Y \subseteq X$: $Y + X \subseteq X + X = X$, поэтому $X + Y = X$. Но и в этом случае Y не будет идемпотентом по той же причине.

Наконец, используя формулу Zero_M, построим $\mathrm{Zero}_1(Z)$, говорящую, что выполнено $\mathrm{Zero}_M(Z)$, а также два следующих условия:

(а) Z — нейтральный или для Z существует как минимум три нейтральных элемента;

(б) для всяких X, Y, для которых выполнено $\mathrm{Zero}_M(X)$ и $\mathrm{Zero}_M(Y)$, из $Y + X = Z$ следует, что $X = Z$ или $Y = Z$.

Пусть $Z = \{0_u\}$. Тогда X и Y должны содержать 0_u и 0_v для некоторого $v \leqslant u$. Но если бы, X и Y содержали 0_v и 0_w для каких-то $v \leqslant w < u$ (или $w \leqslant v < u$), то $X + Y$ будет содержать 0_w (соответственно, 0_v) и, следовательно, $X + Y \neq Z$. Значит, выполнено (б). Условие (а) при $u = 0$ выполнено тривиально, а при $u > 0$ имеем нейтральные для $Z = \{0_u\}$ элементы $\{0_0\}$, $\{0_u\}$, $\{0_0, 0_u\}$,

Пусть теперь выполнено $\mathrm{Zero}_1(Z)$. Предположим, что Z содержит как минимум три элемента: $Z = \{0_u, 0_v, \ldots, 0_w\}$ причём u — наибольший, а w — наименьший возможные, v — второй по величине после u. Тогда получим $\{0_u, 0_w\} + \{0_v, \ldots, 0_w\} = Z$, что противоречит (б).

Рассмотрим теперь вариант, когда Z содержит два элемента: $Z = \{0_u, 0_v\}$, $u > v$. Если $v \neq 0$, то получаем $\{0_u, 0_0\} + \{0_v\} = Z$, что снова противоречит (б). Последний случай: $Z = \{0_u, 0_0\}$, $u > 0$. Но для таких Z существует только два нейтральных элемента: $\{0_0\}$ и само Z, что противоречит (а). □

Заключение

Мы показали, что существует довольно богатый класс полугрупп и моноидов, для которых алгебра всех или только конечных подмножеств имеет разрешимую теорию. При этом очевидным образом из нашего построения следует, что все элементы таких алгебр имеют ограниченный порядок: существует такое натуральное число k, что $ka = 0$.

Первый открытый вопрос, который сразу возникает, — можно ли построить пример полугруппы или моноида, который имел бы элементы сколь угодно больших порядков, но при этом его алгебра подмножеств (или хотя бы конечных подмножеств) имела бы разрешимую теорию.

Второй вопрос, который тоже непосредственно вытекает из предложенной нами конструкции, можно ли найти ещё какой-то «простой» моноид, кроме $\Omega = (\omega, \max, 0)$, для которого теория конечных подмножеств была бы разрешимой. Под простотой мы в данном случае понимаем невозможность его «упрощения» с помощью гомоморфных образов до другого бесконечного моноида.

Список литературы

[1] Дудаков С.М. Об алгоритмических свойствах алгебры конечных подмножеств некоторых уноидов // Вестник ТвГУ. Серия: Прикладная математика. 2019. № 4. С. 108–116. https://doi.org/10.26456/vtpmk550

[2] Blumensath A., Graedel E. Automatic structures // Proceedings of 15th IEEE Symposium on Logic in Computer Science LICS 2000. Los Alamitos, CA, USA: IEEE Computer Society, 2000. Pp. 51–62.

[3] Dudakov S.M. On undecidability of concatenation theory for one-symbol languages // Lobachevskii Journal of Mathematics. 2020. Vol. 40, № 2. Pp. 168–175.

[4] Dudakov S.M. On Undecidability of Subset Theory for Some Monoids // Journal of Physics: Conference Series. 2021. Vol. 1902, № 1. ID 012060. https://doi.org/10.1088/1742-6596/1902/1/012060

[5] Dudakov S., Karlov B. On decidability of theories of regular languages // Theory of Computing Systems. 2021. Vol. 65. Pp. 462–478. http://doi.org/10.1007/s00224-020-09995-4

[6] Dudakov S.M. On Undecidability of Finite Subsets Theory for Torsion Abelian Groups // Mathematics. 2022. Vol. 10, № 3. ID 533.

[7] Rabin M.O. Decidability of second-order theories and automata on infinite trees // Transactions of the American Mathematical Society. 1969. Vol. 141, № 7. Pp. 1–35.

[8] Tamura T., Shafer J. Power semigroups // Mathematicae Japonicae. 1967. Vol. 12. Pp. 25–32.

Образец цитирования

Дудаков С.М. О моноиде с разрешимой теорией конечных подмножеств // Вестник ТвГУ. Серия: Прикладная математика. 2024. №2. С. 27–38. https://doi.org/10.26456/vtpmk708

Сведения об авторах

1. **Дудаков Сергей Михайлович**
декан факультета прикладной математики и кибернетики Тверского госуниверситета; профессор математического факультета НИУ «Высшая школа экономики».

Россия, 170100, г. Тверь, ул. Желябова, д. 33, ТвГУ.
E-mail: sergeydudakov@yandex.ru

ON FINITE SUBSETS MONOID WITH DECIDABLE THEORY

Dudakov S.M.
Tver State University, Tver
HSE University, Moscow

Received 25.04.2024, revised 17.07.2024.

In our previous works, we have proved for various associative algebras that the finite subsets theory allows to interpret elementary arithmetic, in particular, such theory is undecidable. For example, this is proved for all infinite Abelian groups. A natural question arises: can we generalize this result to a wider class of algebras, for example, all commutative monoids. In some cases, we also have proved analogous result: for commutative cancellative monoids with an element of infinite order, or arbitrary Abelian groups. In this paper we prove that this is not true for arbitrary commutative monoids. Moreover, we propose a method that allows to construct such algebras by various original algebras. Also, we have found a limitation of this method.

Keywords: subset algebra, algorithmic decidability, automatic structure.

Citation

Dudakov S.M., "On Finite Subsets Monoid with Decidable Theory", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2024, № 2, 27–38 (in Russian). https://doi.org/10.26456/vtpmk708

References

[1] Dudakov S.M., "On algorithmic properties of finite subset algebra for some unoids", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2019, № 4, 108–116 (in Russian), https://doi.org/10.26456/vtpmk550.

[2] Blumensath A., Graedel E., "Automatic structures", *Proceedings of 15th IEEE Symposium on Logic in Computer Science LICS 2000*, IEEE Computer Society, Los Alamitos, CA, USA, 2000, 51–62.

[3] Dudakov S.M., "On undecidability of concatenation theory for one-symbol languages", *Lobachevskii Journal of Mathematics*, **40**:2 (2020), 168–175.

[4] Dudakov S.M., "On Undecidability of Subset Theory for Some Monoids", *Journal of Physics: Conference Series*, **1902**:1 (2021), 012060, https://doi.org/10.1088/1742-6596/1902/1/012060.

[5] Dudakov S., Karlov B., "On decidability of theories of regular languages", *Theory of Computing Systems*, **65** (2021), 462–478, http://doi.org/10.1007/s00224-020-09995-4.

[6] Dudakov S.M., "On Undecidability of Finite Subsets Theory for Torsion Abelian Groups", *Mathematics*, **10**:3 (2022), 533.

[7] Rabin M.O., "Decidability of second-order theories and automata on infinite trees", *Transactions of the American Mathematical Society*, **141**:7 (1969), 1–35.

[8] Tamura T., Shafer J., "Power semigroups", *Mathematicae Japonicae*, **12** (1967), 25–32.

Author Info

1. **Dudakov Sergey Mikhailovich**
Head of Applied Mathematics and Cybernetics Faculty, Tver State University; Professor of Mathematics Faculty, HSE University.

Russia, 170100, Tver, 33, Zhelyabova str., TverSU.
E-mail: sergeydudakov@yandex.ru